AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A system for providing network-based firewall policy configuration and facilitation associated with a firewall, the system comprising:

a memory device for storing a program for providing the network-based firewall policy configuration and facilitation associated with the firewall; and

a processor, functionally coupled to the memory device, the processor being responsive to computer-executable instructions contained in the program and operative to:

~~a firewall facilitation coordinator configured to~~ receive a first request to add an application not currently supported by a user's firewall policy, ~~and to generate~~

generate a time window during which a user can run the application~~; and~~

~~a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured:~~,

~~to~~ receive a firewall modification request ~~from the firewall facilitation coordinator,~~ to modify the user's firewall policy to allow the application,

~~to~~ determine whether the application includes one or more questionable packets, and

~~to modify~~ if the application is determined to include one or more questionable packets, modify the user's firewall policy to allow ~~at least a portion of the~~ packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the one or more questionable packets associated with the application from modification of the user's firewall policy such that the one or more questionable packets are blocked from passing through the firewall ~~to pass through the firewall unblocked, the at least a portion of the packets associated with the application determined based on whether the application includes one or more questionable packets~~.

2. (Canceled)

3. (Currently Amended) The system of claim 1, wherein the processor is further operative ~~the firewall facilitation coordinator is further configured~~ to decode and decrypt the first

firewall modification request, and ~~further configured~~ to authenticate the user before taking action on the first request.

4-5 (Canceled)

6. (Currently Amended) The system of claim 1, ~~wherein the policy modification agent is further configured to determine whether the firewall modification request is associated with a first attempt to modify the user's firewall policy, and wherein if the application is determined to include one or more questionable packets and the firewall modification request is associated with a first attempt, the at least a portion of the packets associated with the application does not include the one or more questionable packets~~ wherein the processor is further operative to:

receive a second request to add the application; and

modify the user's firewall policy to allow at least a portion of the previously blocked one or more questionable packets associated with the application to pass through the firewall unblocked.

7. (Canceled)

8. (Previously Presented) The system of claim 1, wherein the one or more questionable packets include packets or packet types that are already part of the user's firewall policy or packets previously blocked at times other than during the time window but which are now observed during the time window.

9. (Canceled)

10. (Currently Amended) The system of claim 1, wherein the processor is further operative ~~if the application is determined to include one or more questionable packets, the policy modification agent is further configured~~ to record the one or more questionable packets in a blocking history database if the application is determined to include one or more questionable packets.

11. (Currently Amended) The system of claim 1, wherein the processor is further operative ~~the policy modification agent is further configured~~ to send an acknowledgement to the user ~~via the firewall facilitation coordinator~~ that modification of the user's firewall policy was successful, the acknowledgement including an alert regarding the one or more questionable packets if the application is determined to include the one or more questionable packets.

12. (Currently Amended) The system of claim 1, wherein the processor is further operative ~~the policy modification agent is further configured~~ to:

attempt to modify the user's firewall policy a configurable number of times; and

if unsuccessful, ~~to~~ notify the user to seek assistance or to notify appropriate personnel for assistance.

13. (Currently Amended) The system of claim 1, wherein the processor is further operative ~~if the application is determined to include one or more questionable packet, the policy modification agent is further configured~~ to group the one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets if the application is determined to include one or more questionable packets.

14. (Currently Amended) The system of claim 13, wherein the processor is further operative ~~the policy modification agent is further configured~~ to:

prioritize the groups based on a likelihood that the groups will be required to be added to the user's firewall policy in order to allow the new application to function properly~~, and~~; and

~~to~~ label the groups in order of priority.

15. (Currently Amended) The system of claim 14, wherein the processor is further operative ~~the policy modification agent is further configured~~ to perform successive policy modification attempts to ~~remove one or more of the questionable packet groups previously included in the portion of the packets associated with the application and to add~~ allow one or more of the questionable packet groups previously excluded from modification of the user's

firewall policy having a next highest priority to pass through the firewall unblocked ~~to the portion of the packets associated with the application~~.

16. (Currently Amended) A method for modifying a firewall policy of a network-based firewall, the method comprising:

receiving a first request to modify the firewall policy to incorporate filtering rules to allow packets associated with a new application to pass through the network-based firewall without being blocked;

sending a user an indication of a time window during which the user can exercise the new application;

examining the packets traversing to/from the network-based firewall from/to the user to determine whether the new application includes one or more questionable packets; and

if the new application is determined to include one or more questionable packets, then:

modifying the firewall policy to allow ~~at least a portion of the packets associated with the new application to pass through the network-based firewall unblocked, the at least a portion of the packets associated with the new application determined based on whether the new application includes one or more questionable packets~~ packets associated with the new application determined not to be questionable to pass through the network-based firewall unblocked, and

excluding the one or more questionable packets associated with the new application from modification of the user's firewall policy such that the one or more questionable packets are blocked from passing through the network-based firewall.

17. (Currently Amended) The method of claim 16, further comprising acknowledging the first modification request and sending an acknowledgement of the first modification request to a user's processing device.

18. (Currently Amended) The method of claim 16, further comprising authenticating the user before acting on the first modification request.

19. (Currently Amended) The method of claim 16, further comprising notifying a policy modifier of the first request to modify the firewall policy, wherein notifying the policy modifier further comprises providing a name of the new application and a time frame for modifying the firewall policy.

20. (Previously Presented) The method of claim 16, further comprising sending an acknowledgement of completion of the modification to a user's processing device.

21. (Currently Amended) The method of claim 16, ~~further comprising blocking packets not associated with the filtering rules~~ wherein the one or more questionable packets are associated with an application other than ~~associated with~~ the new application.

22. (Previously Presented) The method of claim 16, wherein the one or more questionable packets include packets or packet types already included in the firewall policy or which were previously blocked at times other than during the time window but which are now observed during the time window.

23. (Currently Amended) The method of claim 16, further comprising: ~~determining whether the request to modify the firewall policy is a first attempt, wherein if the new application is determined to include one or more questionable packets and the request to modify the firewall policy is a first attempt, the at least a portion of the packets associated with the new application does not include the one or more questionable packets~~

receiving a second request to add the new application; and

further modifying the user's firewall policy to allow at least a portion of the previously blocked one or more questionable packets associated with the new application to pass through the network-based firewall unblocked.

24. (Previously Presented) The method of claim 16, further comprising if the new application is determined to include one or more questionable packets, recording the one or more questionable packets in a blocking history database.

25. (Previously Presented) The method of claim 16, further comprising sending an acknowledgement to a user's processing device to repeat an attempt to modify the firewall policy when the new application does not function properly through the network-based firewall after the firewall policy has been modified.

26. (Currently Amended) The method of claim 16, further comprising notifying a user's processing device after a configurable number of repeat attempts fail to modify the firewall policy such that the new application can function properly through the firewall.

27. (Canceled)

28. (Previously Presented) The method of claim 16, further comprising if the new application is determined to include one or more questionable packet, grouping the one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets.

29. (Previously Presented) The method of claim 28, further comprising prioritizing the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function, properly; and labeling the groups in order of priority.

30. (Currently Amended) The method of claim 29, further comprising performing successive policy modification attempts to allow ~~remove~~ one or more of the questionable packet groups previously ~~included in the portion of the packets associated with the new application and to add one or more of the questionable packet groups~~ excluded from modification of the user's firewall policy having a next highest priority to ~~the portion of the packets associated with the new application~~ pass through the network-based firewall unblocked.

31. (Currently Amended) A computer-readable storage medium for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

logic configured to receive a first request to modify a firewall policy to incorporate filtering rules to allow packets associated with a new application to pass through the firewall without being blocked;

logic configured to send a user an indication of a time window during which the user can exercise the new application;

logic configured to examine the packets traversing to/from the firewall from/to the user to determine whether the new application includes one or more questionable packets; and

if the application is determined to include one or more questionable packets, logic configured to modify the firewall policy to allow ~~at least a portion of the~~ packets associated with the new application determined not to be questionable to pass through the firewall unblocked~~, the at least a portion of the packets associated with the new application determined based on whether the new application includes one or more questionable packets~~ and exclude the one or more questionable packets associated with the new application from modification of the firewall policy such that the one or more questionable packets are blocked from passing through the firewall.

32. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to acknowledge the first modification request and logic configured to send an acknowledgement of the first modification request to a user's processing device.

33. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to authenticate the user before acting on the first modification request.

34. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to notify a policy modifier of the first request to modify the firewall policy, the logic configured to notify the policy modifier further configured to provide a name of the new application and a time frame for modifying the firewall policy.

35. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to send an acknowledgement of completion of the modification to a user's processing device.

36. (Currently Amended) The computer-readable storage medium of claim 31, ~~further comprising logic configured to block packets not associated with the filtering rules~~ wherein the one or more questionable packets are associated with an application other than the new application.

37. (Currently Amended) The computer-readable storage medium of claim 31, wherein the one or more questionable packets include packets or packet types already included in the firewall policy or which were previously blocked at times other than during the time window but which are now observed during the time window.

38. (Currently Amended) The computer-readable storage medium of claim 31, further comprising:

logic configured to receive a second request to add the new application; and

logic configured to modify the firewall policy to allow at least a portion of the previously blocked one or more questionable packets associated with the new application to pass through the firewall unblocked.

39-40 (Canceled)

41. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to record the one or more questionable packets in a blocking history database if the new application is determined to include one or more questionable packets.

42. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to send an acknowledgement to a user's processing device to repeat an attempt to modify the firewall policy when the new application does not function properly through the firewall after the firewall policy has been modified.

43. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to notify a user's processing device after a configurable number of repeat attempts fail to modify the firewall policy such that the new application functions properly through the firewall.

44. (Canceled)

45. (Currently Amended) The computer-readable storage medium of claim 31, further comprising logic configured to group the one or more questionable packets into one or more groups based on a type associated with the one or more questionable packets if the new application is determined to include one or more questionable packets.

46. (Currently Amended) The computer-readable storage medium of claim 45, further comprising logic configured to prioritize the groups based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly, and to label the groups in order of priority.

47. (Currently Amended) The computer-readable storage medium of claim 46, further comprising logic configured to perform successive policy modification attempts to ~~remove~~ allow one or more of the questionable packet groups previously ~~included in the portion of the packets associated with the new application and to add one or more of the questionable packet groups~~ excluded from modification of the firewall policy having a next highest priority to ~~the portion of the packets associated with the new application~~ pass through the firewall unblocked.

48. (Currently Amended) A system for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

a memory device for storing a program for providing the network-based firewall policy configuration and facilitation associated with the firewall; and

a processor, functionally coupled to the memory device, the processor being responsive to computer-executable instructions contained in the program and operative to:

~~a firewall facilitation coordinator configured to~~ receive a request to add an application not currently supported by a user's firewall policy, ~~and to~~

generate a time window during which a user can run the application~~;~~,

~~a policy modification agent adapted to communicate with the firewall facilitation coordinator, the policy modification agent configured to receive a firewall modification request from the firewall facilitation coordinator, to be aware of communications or packets observed by the firewall during the time window, and to modify the user's firewall policy; and~~

~~a blocking history checker for checking the communications or~~ check packets observed during the time window to be associated with the application ~~in order to identify~~ to determine whether the packets include one or more questionable ~~communications or packets~~ packets ~~which are defined as those communications/packets or communications/packet types that are already part of the user's firewall policy or communications or packets previously blocked at times other than during the time window but which are now observed during the time window~~,

when the application is determined to include one or more questionable packets, group the one or more questionable packets by type,

prioritize groups of the one or more questionable packets ~~wherein the policy modification agent is further configured to group the types of questionable packets singly and in combination of two or more, and to prioritize the groups~~ based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the ~~new~~ application to function properly~~, and to label the groups in order of priority~~, and

modify the user's firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked and exclude the groups of the one or more questionable packets associated with the application from modification of the user's firewall policy such that the groups of the one or more questionable packets are blocked from passing through the firewall.

49. (Currently Amended) The system of claim 48, wherein the processor is further operative ~~the policy modification agent is further configured~~ to perform successive policy modification attempts to ~~remove~~ allow one or more of the ~~questionable packet~~ groups of the one or more questionable packets previously excluded from modification of the user's firewall policy

to pass through the firewall unblocked, ~~previously added questionable packet groups and to add the next highest priority group to the firewall policy~~ an order of the one or more groups allowed to pass through the firewall unblocked based on a priority associated with each of the one or more groups.

50. (Currently Amended) A method for modifying a firewall policy of a network-based firewall, comprising:

notifying a coordinating entity of a request to modify the firewall policy to incorporate filtering rules to allow ~~communications or~~ packets from a new application to pass through the network-based firewall without being blocked;

notifying a policy modifier of the modification request;

sending a user an indication of a time window during which the user can exercise the new application;

examining the ~~communications or~~ packets traversing to/from the network-based firewall from/to the user ~~and modifying the user's firewall policy such that necessary communications or packets associated with the new application are allowed to pass through the network-based firewall; and~~

~~inspecting received communications or packets and checking a blocking history to identify questionable communications or packet types which are defined as those communications/packet types observed during the time window to be associated with the application but which are already included in the firewall policy or communications/packet types which were previously blocked at times other than during the time window but which are now observed during the time window,~~ to determine whether the packets include one or more questionable packets;

when the application is determined to include one or more questionable packets, grouping the one or more questionable packets by type;

~~wherein examining the communications or packets further comprises grouping the types of questionable packets singly and in combination of two or more, and~~

~~wherein examining the communications or packets further comprises~~ prioritizing ~~the~~ groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly; ~~, and labeling the groups in order of priority~~

modifying the firewall policy to allow packets associated with the application determined not to be questionable to pass through the firewall unblocked; and

excluding the groups of the one or more questionable packets associated with the application from modification of the firewall policy such that the groups of the one or more questionable packets are blocked from passing through the firewall.

51. (Currently Amended) The method of claim 50, wherein examining the ~~communications or~~ packets further comprises performing successive policy modification attempts to ~~remove~~ ~~previously added questionable packet~~ allow one or more of the groups of the one or more questionable packets previously excluded from modification of the firewall policy to pass through the network-based firewall unblocked, ~~and adding the next highest priority group to the firewall policy~~ an order of the one or more groups allowed to pass through the firewall unblocked based on a priority associated with each of the one or more groups.

52. (Currently Amended) A computer-readable storage medium for providing network-based firewall policy configuration and facilitation associated with a firewall, comprising:

logic configured to notify a coordinating entity of a request to modify a firewall policy to incorporate filtering rules to allow ~~communications or~~ packets from a new application to pass through the ~~network-based~~ firewall without being blocked;

logic configured to notify a policy modifier of the modification request;

logic configured to send a user an indication of a time window during which the user can exercise the new application;

logic configured to examine the ~~communications or~~ packets traversing to/from the firewall from/to the user ~~and modifying the user's firewall policy such that necessary communications or packets associated with the new application are allowed to pass through the firewall;~~

~~logic configured to inspect received packets;~~

~~logic configured to check blocking history to identify questionable communications or packet types which are defined as those communications or packet types~~

~~already included in the firewall policy or communications or packet types which were previously blocked at times other than during the time window but which are now observed during the time window~~ to determine whether the packets include one or more questionable packets;

when the packets are determined to include one or more questionable packets, logic configured to group ~~the types of questionable packets singly and in combination of two or more~~ the one or more questionable packets by type; ~~and~~

logic configured to prioritize ~~the~~ groups of the one or more questionable packets based on a likelihood that the groups will be required to be added to the firewall policy in order to allow the new application to function properly~~, and to label the groups in order of priority~~; and

logic configured to modify the firewall policy to allow packets associated with the new application determined not to be questionable to pass through the firewall unblocked and to exclude the groups of the one or more questionable packets associated with the new application from modification of the user's firewall policy such that the groups of the one or more questionable packets are blocked from passing through the firewall.

53. (Currently Amended) The computer-readable storage medium of claim 52, further comprising logic configured to perform successive policy modification attempts to ~~remove previously added~~ allow one or more of the groups of the one or more questionable ~~packet groups~~ packets previously excluded from modification of the firewall policy to pass through the firewall unblocked, ~~and to add the next highest priority group to the firewall policy~~ an order of the one or more groups allowed to pass through the firewall unblocked based on a priority associated with each of the one or more groups.